REMARKS

Claims 1-23 are pending in the application.

The specification is objected to as failing to provide proper antecedent basis for the preamble "machine-executable medium" language of claims 15-21.

Claims 1-23 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ananian et al. (US 2003/0028451) in view of Boyce et al. (6,934,838).

Applicant hereby amends the claims to overcome the objections and the rejections, and submits that all pending claims now are allowable. Specifically, applicant amends the specification to provide antecedent basis for the objected-to language consistent with the application as originally filed, thus adding no new matter (see, for example, Paragraphs [00018], [00020], [00025]; original claim 15; and Figs. 2-4). Applicant also makes certain other changes to the claims more definitely to recite applicant's invention and to make them read better so that all claims readily are deemed allowable.

Claim Rejections – 35 U.S.C. § 103

Claims 1-23 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ananian et al. in view of Boyce et al.

First, applicant submits that neither Ananian nor Boyce, nor their combination, teaches all elements of applicant's amended claims including the limitation wherein a resident application manages access to a subject's personal record in an unencrypted state "by use of a security element including an encrypted private key securely accessible only to the subject such that the encrypted private key *is inaccessible to the anonymity service...*" (amended claims 1 and 8) or "*is inaccessible to others*" (amended claim 15). Thus applicant's claims even more definitely recite applicant's invention and its contribution providing security against unauthorized access to private subject data.

As submitted previously, applicant's invention focuses on an untrustworthy anonymity server model wherein the anonymity server itself is denied access to a subject's private data. This is a great advance beyond the teachings of Ananian and Boyce. Ananian preserves a user's anonymity, but *freely shares* information related to the user's profile with vendors. (Fig. 17, block 2514; paragraph [0537]). Moreover, Ananian's Catalog Server System 200 entrusted with user profile information is stored in a Personal Asset Data Store (PAD) that is *remote* from the user rather than residing in the client device under control of the user. Clearly, Ananian does not teach rendering an encrypted private key inaccessible to

Docket No. 104015-0003   Page 9 of 12   Application No. 10/772,202

PAGE 11/14 * RCVD AT 4/27/2009 5:40:27 PM [Eastern Daylight Time] * SVR:USPTO-EFXRF-5/28 * DNIS:2738300 * CSID:5032260079 * DURATION (mm-ss):02-12

an anonymity service. Nor does Boyce come to Ananian's assistance. As argued previously, *all the information needed to obtain Boyce's User 12's security credentials, including Boyce's User 12's private key*, remains indefinitely available to Boyce's Service Provider 20. Boyce fails to specify whether or how his Service Applications 40 would be denied access to his User 12's private key. In any event, Boyce's Service Provider 20 is clearly and unambiguously regarded as a trusted intermediary where security credentials are concerned.

Moreover, applicant hereby amends claims 1, 8, 9, 12, 15, 16, and 19 even more clearly and distinctly to recite his invention.

Independent claim 1 as amended hereby expressly recites a secure messaging system that features "a security element including an encrypted private key" to manage access to a personal record in an unencrypted state, the resident application residing on a client device under control of the subject. It also expressly recites that "the resident application, the quarantine memory and the session agent all reside *on the client device under control of the subject*" and that "the resident application, the quarantine memory and the session agent collectively secure the personal record and the private key *in an unencrypted state against access by the anonymity service*." (Emphasis added.)

Neither Ananian nor Boyce teach such recited elements in combination, whether considered alone or for any teachings motivated by them in their combination.

The Examiner is reminded that Boyce teaches sending user initialization data including a stored user identifying secret to a service registration application (SRA) 22 and mapping repository 26 that are remote from the user rather than being on the user device. (Column 6, lines 4-27.) In Boyce's perfect world (under the auspices of Entrust Technologies Ltd.), server-side-resident "trusted" or "entrusted" or "trustworthy" service providers including anonymity servers are all equally trusted with user profile and secret information including private signing and/or encryption keys.

This in stark contrast to the invented quarantining of the same in a memory residing and maintained inaccessible to the anonymity server and others at the client device under the exclusive control of the subject whose privacy is to be trusted to no one else. See Paragraphs [00010], [00019], [00021], [00022], [00028], and [00032] ("Each of the transmissions between Anonymity Service 130 and Resident Application 121 are sent with various levels of encryption to protect the *privacy of the data* and *the anonymity of Subject 120.*" With Ananian and Boyce, it is at best one or the other, not both.) Thus, applicant submits that claim 1, as amended, along with claims 2-7, 22, and 23 depending therefrom and further distinguishing over the record prior art, is allowable.

Docket No. 104015-0003   Page 10 of 12   Application No. 10/772,202

Applicant notes that claim 23, for example, further expressly recites that the quarantine memory contents including the personal record and the private key *"are deleted* at an end of the client session." (Emphasis added.) The Examiner asserts at page 10 of the Office action deemed final that such is taught by Boyce at column 8, lines 48-55. Applicant respectfully submits that the Examiner is simply mistaken, in this and other regards.

Boyce says only that access requests "provide no direction information about the user or the user's information (e.g. bank account number), thereby making the data useless to a hacker." Camouflaging certain stored information that might be useful to a hacker (a la Boyce) is not the same as (nor does it render obvious) the invented fail-safe *deletion* of such private information-containing contents from a quarantine memory at the end of a client session (a la Thorson).

Applicant respectfully submits that this wishful or careless reading of Boyce is factual error and that the rejection of claim 23 based thereon is legal error.

Independent claim 8 as amended hereby expressly recites a secure messaging method that features a database operation performed on a personal record in an unencrypted form in "a quarantine memory at the client device by use of a security element *including an encrypted private key securely maintained by and accessible only to the subject such that the encrypted private key is inaccessible to the anonymity service."* (Emphasis added.)

Neither Ananian nor Boyce teach the recited element, whether alone or in combination, without the use of impermissible hindsight by the Examiner in view of applicant's invention disclosure. Thus, applicant submits that claim 8, as amended, along with claims 9-14 depending therefrom and further distinguishing over the record prior art, is allowable.

Independent claim 15 as amended hereby expressly recites a machine-executable medium comprising instructions that when executed cause the machine to distribute a database operation from a centralized database to a client device, wherein the database operation is performed on the personal record in an unencrypted form in "a quarantine memory at the client device by use of a security element *including an encrypted private key securely maintained by and accessible only to the subject such that the encrypted private key is inaccessible to all others."* (Emphasis added.)

Neither Ananian nor Boyce, alone or in combination, teach the recited element of excluding access to an encrypted private key by all others but to the subject about whom the personal record pertains. Thus, applicant submits that claim 15, as amended, along with
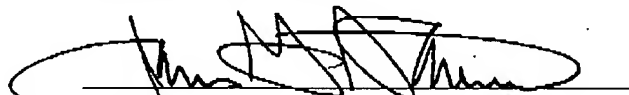
Docket No. 104015-0003   Page 11 of 12   Application No. 10/772,202

PAGE 13/14 * RCVD AT 4/27/2009 5:40:27 PM [Eastern Daylight Time] * SVR:USPTO-EFXRF-5/28 * DNIS:2738300 * CSID:5032260079 * DURATION (mm-ss):02-12

claims 16-21 depending therefrom and further distinguishing over the record prior art, is allowable.

CONCLUSION

Applicant submits that this amendment should be entered after final Office Action because its amendments present the rejected claims in proper form for allowance; at the most requires only straightforward reconsideration by the Examiner; and at the least removes or simplifies issues on appeal, if needed.

Accordingly, applicant requests entry of the above amendment and allowance of the application on the merits. The Examiner is encouraged to telephone the undersigned at (503) 226-1191 if it appears that an interview would be helpful in advancing the case.
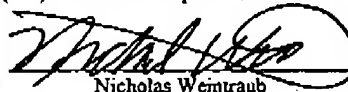
Respectfully submitted,

James G. Stewart
Reg. No. 32,496
Ater Wynne LLP
1331 NW Lovejoy Street, Suite 900
Portland, Oregon 97209

Customer No. 35940

I hereby certify that this correspondence is being transmitted to the U.S. Patent and Trademark Office via facsimile number (571) 273-8300 on April 27, 2009.

Nicholas Weintraub

Docket No. 104015-0003   Page 12 of 12   Application No. 10/772,202

PAGE 14/14 * RCVD AT 4/27/2009 5:40:27 PM [Eastern Daylight Time] * SVR:USPTO-EFXRF-5/28 * DNIS:2738300 * CSID:5032260079 * DURATION (mm-ss):02-12